Cyren Incident Response Service (CIRS)

Sicher und sorglos kommunizieren: Profitieren Sie von Cyrens Services für Office 365

Mit dem Cyren Incident Response Service (CIRS) entlasten Sie Sicherheitsteams, die von Cyberwarnungen überschwemmt werden und Schwierigkeiten haben, Bedrohungen zu untersuchen und zu beseitigen. Dank CIRS-Beratern, die fortlaufend Ausschau nach verdächtigen E-Mails, Mailboxanomalien und Cybertrends halten, können Sie mit einer schnellen und effektiven Reaktion auf böswillige Angriffe rechnen, die Ihre Office-365-Anwender und Ihr Unternehmen gefährden.

Selbst Evasive-Phishing-Angriffe, die immer wieder ihre Gestalt und Herangehensweise ändern, hat unser Team aus CIRS-Experten nichts entgegenzusetzen. Bevor Ihr IT-Team die Zeit findet, sich eine verdächtige E-Mail anzusehen, hat CIRS sie im Normalfall bereits untersucht, den Vorfall geklärt und die entsprechende Reaktion veranlasst. Darüber hinaus nutzen wir unsere Erfahrung mit einer Vielzahl von Cyberangriffen über zahlreiche Organisationen und Branchen hinweg, um Ihnen dabei zu helfen, den Überblick über Angriffsvektoren zu behalten, die Ihr Geschäft bedrohen. Gleichzeitig stellen wir sicher, dass gemeldete Vorfälle umgehend behandelt und Sicherheitsverletzungen verhindert werden.

Wie geht Cyren dabei vor? Kurz gesagt: mit dem richtigen Know-how.

Schneller reagieren dank fundierter Expertise

CIRS ist eine rund um die Uhr bereitgestellte Dienstleistung für Nutzer von Cyren Inbox Security. Unsere Bedrohungsexperten konzentrieren sich vollständig auf die Untersuchung, Analyse und Lösung von Bedrohungsvorfällen, die von Ihren Office 365 Postfachbenutzern gemeldet werden, sowie auf die Untersuchung von verdächtigen Low-Confidence-Vorfällen, die vom CIS-System erkannt wurden.

Wir nutzen unsere unübertroffene Bedrohungstransparenz und Cyrens eigens entwickeltes Toolset, um Ihre IT-Mitarbeiter zu entlasten und Ihnen die Sorge vor Sicherheitsvorfällen in Office 365 zu nehmen. Unsere globale Sicherheitscloud verarbeitet 25 Milliarden E-Mail- und Websicherheitstransaktionen pro Tag, erkennt 9 neue Bedrohungen und blockiert über 3.000 bekannte Bedrohungen pro Sekunde. Cyren sammelt mit jedem untersuchten und gelösten Vorfall neue Erfahrung und Expertise. Wir haben schon alles gesehen. Während wir unsere globale Präsenz und durch Crowdsourcing gewonnene Erkenntnisse zum Vorteil aller Nutzer von Cyren Inbox Security weltweit verwenden, sind die CIRS-Sicherheitsanalysten speziell dafür zuständig, auf die gemeldeten Vorfälle aus Ihrem Unternehmen zu reagieren und sie zeitnah zu lösen.

Liegt eine echte Bedrohung vor?

Wenn ein Nutzer von Cyren Inbox Security auf die rote PhishScan-Schaltfläche klickt, um eine verdächtige E-Mail zu melden, kann sie in eine von drei Kategorien fallen:

- Phishing-Bedrohung, die von CIS erkannt wurde, aber keine ist
- Phishing-Bedrohung, die nicht von CIS erkannt wurde, aber hätte erkannt werden müssen
- Unerwünschte E-Mail (an sich keine Sicherheitsbedrohung, aber unerwünscht oder lästig)

Jeder Bedrohungsbericht wird umgehend von CIRS-Experten untersucht und überprüft, um festzustellen, ob die gemeldete Bedrohung echt ist oder nicht. Bestätigte Bedrohungen können einen automatischen Rescan oder eine Remediation aller Postfächer auslösen, um beispielsweise einen Phishing-Angriff zu unterbinden. Wenn eine gemeldete Bedrohung sich nicht als echt erweist, wird der Vorfall sofort gelöst und abgeschlossen.

CYREN INBOX SECURITY

Cyren Inbox Security ist eine Lösung für Inbox Detection and Response (IDR), mit der Organisationen eine kritische Sicherheitsebene im Posteingang einrichten und ihre gesamte Sicherheitsaufstellung stärken können.

INCIDENT RESPONSE SERVICE

Mit dem Cyren Incident Response Service werden unsere versierten Sicherheitsanalysten zu einem wesentlichen Bestandteil Ihres Office 365-Sicherheitsteams. Im Rahmen dieses rund um die Uhr verwalteten Dienstes stehen die Sicherheitsexperten von Cyren für Sie bereit, um verdächtige E-Mails zu prüfen und darauf zu reagieren, wenn ein Mitarbeiter auf die rote PhishScan-Schaltfläche klickt.

KOMPETENTE GEFAHRENANALYSE

Ihre Sicherheit in Expertenhände zu legen, zahlt sich aus. Die Cyren Incident Response Analysten verfügen über umfangreiches Wissen im Bereich Cybersicherheit, das von keiner automatisierten, maschinellen Überprüfung erreicht werden kann.

CIRS HILFT IHNEN DABEI:

- Ihr SOC (Sicherheitsoperationszentrale) Team von der komplizierten und stressigen Untersuchung von und Reaktion auf Bedrohungen zu befreien
- Ihre SOC durch die von Cyren verwalteten Dienste mit Wissen und Ressourcen im Bereich Cybersicherheit auszustatten
- Melderückstaus und Übermüdung zu reduzieren
- Sicherzustellen, dass Mitarbeiter eine zeitnahe Antwort auf Ihre PhishScan-Meldungen erhalten
- Sich verändernde Umgehungstaktiken festzustellen, wenn Angreifer umschwenken und neue Techniken einsetzen
- Sicherzustellen, dass jede Bedrohung geklärt und keine Meldung übersehen wird

25 Mrd.
Sicherheitstransaktionen pro Tag

1,3 Mrd.
geschützte Benutzer

300 Mio.
abgewehrte Gefahren pro Tag

Schnelle Behebung von Sicherheitsvorfällen

Jeden Tag untersuchen und beheben Analysten vom Cyren Incident Response Service (CIRS) zahlreiche Vorfälle wie diese:

PHISHING AUF DEM SHAREPOINT

- Ein Mitarbeiter meldet eine verdächtige E-Mail per PhishScan.
- CIRS bestätigt Phishing unter Verwendung einer URL, auf die von einer auf dem SharePoint des Unternehmens geöffneten Datei aus zugegriffen wird.
- Phishing-URL wird manuell blockiert. Nachfolgende Angriffe werden bereits beim Eintreffen erkannt und automatisch abgewehrt.

PHISHING-ANGRIFF AUF GETRÄNKEHERSTELLER

- CIRS erkennt Phishing-Angriff auf ein bestimmtes Nutzerkonto
- Der Angriff wird innerhalb von 4 Minuten bestätigt und die angreifende URL wird im betroffenen Nutzerkonto und in 22 weiteren Konten blockiert.
- Acht nachfolgende Angriffe werden bereits beim Eintreffen erkannt und automatisch abgewehrt.
- Globaler Hersteller; mehr als 10.000 Mitarbeiter.

BETRUGSVERSUCH IN UNIVERSITÄT

- Universitätsnutzer fordert einen PhishScan für eine E-Mail mit verdächtigem Inhalt und Absender an.
- CIRS erkennt betrügerische Werbesendung, die wiederholt an alle Universitätsmitarbeiter geschickt wurde. Keine Phishing-Bedrohung, aber lästig und unerwünscht.
- Der Absender wird auf die schwarze Liste gesetzt, während IOCs (Indicators of Compromise) der Cyren Inbox Security KI Detection Engine zugeführt werden
- 450+ Konten geschützt. Nachfolgende Betrugsmails (neue Absenderadresse) werden bereits beim Eintreffen erkannt und automatisch abgewehrt.

KOMPROMITTIERTES KONTO

- Mitarbeiter erhalten sonderbare E-Mail vom „Microsoft Outlook HelpDesk“ mit einer bösartigen URL
- Cyren Inbox Security identifiziert Phishing-Versuch und versieht die E-Mail mit einer Warnmeldung
- CIRS erkennt, dass Angriff von einem legitimen Nutzerkonto erfolgte, das kompromittiert ist
- CIRS benachrichtigt Sicherheitsteam des Kunden über kompromittiertes Konto.

Cyrens professionelle Playbooks automatisieren und beschleunigen die Reaktion auf Sicherheitsvorfälle

Mit CIRS-Playbooks wird die Untersuchung von und Reaktion auf jede Art von Phishing-Bedrohung, die Ihren Office 365-Nutzern begegnen kann, gesteuert und automatisiert:

1. Analyse des Cybervorfalls, um den Umfang des Angriffs zu ermitteln
2. Identifizierung und Meldung von potentiell kompromittierten Daten und ihren Auswirkungen
3. Festlegung von Anforderungen für eine vollständige forensische Untersuchung
4. Entwicklung eines Remediationsplans basierend auf dem Umfang und den Details des Cybervorfalls
5. Fall beheben und als abgeschlossen melden
6. Senden des Vorfallberichts an den Administrator